

GIBSON, DUNN & CRUTCHER LLP
LAUREN R. GOLDMAN (admitted *pro hac vice*)
MICHAEL BRANDON (admitted *pro hac vice*)
200 Park Avenue
New York, NY 10166
Telephone: (212) 351-4000
Facsimile: (212) 351-4035
lgoldman@gibsondunn.com
mbrandon@gibsondunn.com

CHRISTOPHER CHORBA, SBN 216692
ABIGAIL A. BARRERA, SBN 301746
EMILY SAUER, SBN 324695
333 South Grand Avenue
Los Angeles, CA 90071
Telephone: (213) 229-7396
Facsimile: (213) 229-6396
cchorba@gibsondunn.com
abarrera@gibsondunn.com
esauer@gibsondunn.com

LUCAS TOWNSEND (admitted *pro hac vice*)
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036
Telephone: (202) 955-8500
Facsimile: (202) 467-0539
ltownsend@gibsondunn.com

Attorneys for Defendant Meta Platforms, Inc.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

NATALIE TURCK, individually and on behalf
of all others similarly situated,

Plaintiff,

v.

META PLATFORMS, INC.,

Defendant.

Case No. 3:23-cv-04181-SI

**DEFENDANT META PLATFORMS,
INC.'S MOTION TO DISMISS
PLAINTIFF'S COMPLAINT**

*[Declaration of Christopher Chorba and
Exhibits A–F; Request for Incorporation by
Reference or Judicial Notice filed
concurrently herewith]*

Action Filed: August 16, 2023
Hearing Date: February 2, 2024
Trial Date: None Set
Judge Susan Illston

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE THAT on February 2, 2024, at 10 a.m., or as soon thereafter as the matter may be heard before the Honorable Susan Illston, in Courtroom 1, 17th Floor, of the United States District Court for the Northern District of California in the San Francisco Courthouse, 450 Golden Gate Avenue, San Francisco, CA 94102, Defendant Meta Platforms, Inc. (“Meta”) will, and hereby does, move this Court, pursuant to Rules 8(a) and 12(b)(6) of the Federal Rules of Civil Procedure, for an Order dismissing the complaint on several grounds:

First, Plaintiff Natalie Turck’s binding agreement that California law shall govern all disputes with Meta arising from her use of Meta’s services bars her claims against Meta under Illinois’ Biometric Information Privacy Act (“BIPA”). Ms. Turck alleges that Meta collected her voiceprint after she input her voice recording into Meta’s Facebook and Messenger services, and her claims arise from her use of those services. The parties’ valid choice-of-law clause applies and forecloses Ms. Turck’s ability to sue Meta for claims under Illinois law.

Second, even if the Court were to apply Illinois law in this case, Ms. Turck has not stated any plausible claim for relief. BIPA regulates companies’ collection and possession of sensitive biometric data, such as “voiceprints”—i.e., data generated from a voice recording that is used to uniquely identify the individual speaker; BIPA does not regulate the collection or possession of mere voice recordings themselves. Ms. Turck has not alleged any facts that plausibly suggest that Meta collected her voiceprint—either through Facebook or Messenger or from third parties—as opposed to her voice recording.

The complaint relies entirely on two sources as purported support for Ms. Turck’s conclusory assertion that Meta collected her voiceprint: (1) a patent and its continuations that Meta owns indicating that Meta would have intellectual property protections if it *were* to collect a person’s voiceprint in a particular way through a hypothetical “social networking system,” and (2) a statement in Meta’s United States Regional Privacy Notice stating that Meta may collect users’ voice recordings that could be used to identify them. Neither of these sources provides plausible support for the allegation that Meta has collected *any* voiceprints. The existence of a patent does not indicate that the owner practices the covered invention, and Meta’s U.S. Regional Privacy Notice merely reflects—

1 consistent with Meta’s disclosure obligations under California law—that Meta may collect a *voice*
2 *recording*—not a *voiceprint*—from users of its services. Further, even if these sources did suggest that
3 Meta collects some voiceprints, Ms. Turck alleges no facts suggesting that Meta collected *her*
4 voiceprint through her use of Facebook and Messenger. And her theory that Meta may have collected
5 her voiceprint from audio obtained from unnamed “third parties” is even more speculative. Ms. Turck
6 cannot plausibly place her voice in any such third-party audio, much less plausibly allege that Meta
7 then created her voiceprint from that third-party audio.

8 *Third*, even if Ms. Turck did plausibly allege that Meta collected voiceprints under BIPA, her
9 complaint still fails to plausibly allege claims against Meta under BIPA Sections 15(c) and 15(e),
10 because she has not pleaded any facts that show Meta “profited” from her biometric data within the
11 meaning of Section 15(c) or failed to store that data with the care required under Section 15(e). For
12 these independent reasons, the Court should dismiss Ms. Turck’s BIPA claims against Meta under
13 Sections 15(c) and 15(e).

14
15 Dated: October 25, 2023

GIBSON, DUNN & CRUTCHER LLP

16 By: /s/ Christopher Chorba
17 Christopher Chorba

18 *Attorneys for Meta Platforms, Inc.*
19
20
21
22
23
24
25
26
27
28

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. FACTUAL BACKGROUND	3
III. LEGAL STANDARD	6
IV. ARGUMENT	6
A. The BIPA Claims Are Barred By The California Choice-Of-Law Clause To Which Ms. Turck Agreed In Meta's Terms Of Service	6
1. Ms. Turck Is Bound By The California Choice-Of-Law Clause In Meta's Terms Of Service	6
2. The California Choice-Of-Law Clause Bars Ms. Turck's Claims Under BIPA	8
B. Even If Illinois Law Applies, Ms. Turck's BIPA Claims Fail Because They Are Conclusory And Speculative	13
1. Plaintiff Does Not Plausibly Allege That Meta Collects Voiceprints From Anyone	14
2. Ms. Turck Does Not Plausibly Allege That Meta Collected <i>Her</i> Voiceprint	17
3. Ms. Turck Does Not Plausibly Allege That Meta Collected Her Voiceprint From Audio Recordings Provided By Any Third Party	19
C. Ms. Turck's BIPA Claims For Profiting And Storage Fail For Additional Reasons	20
1. Ms. Turck Has Not Plausibly Alleged That Meta Profits From Her Voiceprint	20
2. Ms. Turck Has Not Plausibly Alleged That Meta Failed To Exercise Reasonable Care In Storing Her Voiceprint	22
V. CONCLUSION	23

TABLE OF AUTHORITIES

Page(s)

Cases

<i>A.C.L. Computers & Software, Inc. v. United States</i> , 727 F. App'x 376 (9th Cir. 2018)	14
<i>In re Apple Inc. Device Performance Litig.</i> , 347 F. Supp. 3d 434 (N.D. Cal. 2018)	8
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)	6, 15, 18, 23
<i>Bell Atlantic Corp. v. Twombly</i> , 550 U.S. 544 (2007)	6, 19, 23
<i>Brazil v. Dell Inc.</i> , 585 F. Supp. 2d 1158 (N.D. Cal. 2008)	9
<i>Carpenter v. McDonald's Corp.</i> , 580 F. Supp. 3d 512 (N.D. Ill. 2022)	14
<i>Casey v. Toyota Motor Eng'g & Mfg. N. Am., Inc.</i> , 770 F.3d 322 (5th Cir. 2014)	15
<i>In re Century Aluminum Co. Sec. Litig.</i> , 729 F.3d 1104 (9th Cir. 2013)	6, 13, 14, 15
<i>Colaco v. Cavotec SA</i> , 25 Cal. App. 5th 1172 (2018)	8
<i>Ctr. for Biological Diversity v. Bernhardt</i> , 946 F.3d 553 (9th Cir. 2019)	19
<i>Davis v. Meta Platforms, Inc.</i> , No. 4:22-cv-01001, 2023 WL 4670491 (E.D. Tex. July 20, 2023)	7
<i>Dep't of Educ. v. Brown</i> , 600 U.S. 551 (2023)	20
<i>Dolin v. Facebook, Inc.</i> , 289 F. Supp. 3d 1153 (D. Haw. 2018)	7
<i>Eclectic Props. E., LLC v. Marcus & Millichap Co.</i> , 751 F.3d 990 (9th Cir. 2014)	14
<i>Emblaze Ltd. v. Apple Inc.</i> , No. 5:11-cv-01079-PSG, 2015 WL 396010 (N.D. Cal. Jan. 29, 2015)	16
<i>In re Facebook Biometric Info. Privacy Litig.</i> , 185 F. Supp. 3d 1155 (N.D. Cal. 2016)	8, 11, 12
<i>Frenzel v. Aliphcom</i> , No. 14-cv-03587-WHO, 2015 WL 4110811 (N.D. Cal. July 7, 2015)	8

1	<i>Fteja v. Facebook, Inc.</i> ,	
2	841 F. Supp. 2d 829 (S.D.N.Y. 2012).....	7
3	<i>Gershzon v. Meta Platforms, Inc.</i> ,	
4	No. 23-cv-00083-SI, 2023 WL 5420234 (N.D. Cal. Aug. 22, 2023)	5
5	<i>Gonzalez v. Planned Parenthood of L.A.</i> ,	
6	759 F.3d 1112 (9th Cir. 2014).....	13, 14
7	<i>Hayes v. Facebook</i> ,	
8	No. 18-cv-02333-MEH, 2019 WL 8275335 (D. Colo. Mar. 6, 2019).....	7
9	<i>Heard v. Becton, Dickinson & Co.</i> ,	
10	440 F. Supp. 3d 960 (N.D. Ill. 2020)	20, 23
11	<i>Jones v. Microsoft Corp.</i> ,	
12	___ F. Supp. 3d ___, 2023 WL 130495 (N.D. Ill. Jan. 9, 2023).....	23
13	<i>King Instruments Corp. v. Perego</i> ,	
14	65 F.3d 941 (Fed. Cir. 1995).....	16
15	<i>Kloss v. Acuant, Inc.</i> ,	
16	462 F. Supp. 3d 873 (N.D. Ill. 2020)	20
17	<i>LeBoeuf v. NVIDIA Corp.</i> ,	
18	No. 19-cv-03543-SVK, 2019 WL 13210428 (N.D. Cal. Nov. 18, 2019).....	8, 9
19	<i>Loomer v. Facebook, Inc.</i> ,	
20	No. 19-cv-80893, 2020 WL 2926357 (S.D. Fla. Apr. 13, 2020)	7
21	<i>Loveland v. Facebook</i> ,	
22	No. 20-cv-6260-JMY, 2021 WL 1734800 (E.D. Pa. May 3, 2021)	7
23	<i>MaxLite, Inc. v. ATG Electronics, Inc.</i> ,	
24	No. 8:20-cv-01056-MCS-ADS, 2022 WL 16923391 (C.D. Cal. Aug. 7, 2022)	12
25	<i>McGoveran v. Amazon Web Servs., Inc.</i> ,	
26	No. 1:20-cv-01399-SB, 2023 WL 2683553 (D. Del. Mar. 29, 2023).....	14
27	<i>Menzel v. Scholastic, Inc.</i> ,	
28	No. 17-cv-05499-EMC, 2018 WL 1400386 (N.D. Cal. Mar. 19, 2018).....	19
	<i>Miller v. Facebook, Inc.</i> ,	
	No. 1:09-cv-2810-RLV, 2010 WL 9525523 (N.D. Ga. Jan. 15, 2010)	7
	<i>Namuwonge v. Kronos, Inc.</i> ,	
	418 F. Supp. 3d 279 (N.D. Ill. 2019)	18, 23
	<i>Nedlloyd Lines B.V. v. Super. Ct.</i> ,	
	3 Cal. 4th 459 (1992)	8, 9, 13
	<i>Nguyen v. Barnes & Noble Inc.</i> ,	
	763 F.3d 1171 (9th Cir. 2014).....	7

1	<i>Palomino v. Facebook, Inc.</i> ,	
2	No. 16-cv-04230-HSG, 2017 WL 76901 (N.D. Cal. Jan. 9, 2017)	8, 11
3	<i>Pfaff v. Wells Elecs., Inc.</i> ,	
4	525 U.S. 55 (1998)	16
5	<i>Rite-Hite Corp. v. Kelley Co.</i> ,	
6	56 F.3d 1538 (Fed. Cir. 1995)	16
7	<i>Rivera v. Google Inc.</i> ,	
8	238 F. Supp. 3d 1088 (N.D. Ill. 2017)	3, 14
9	<i>Rojas-Lozano v. Google, Inc.</i> ,	
10	159 F. Supp. 3d 1101 (N.D. Cal. 2016)	11
11	<i>Scott v. Experian Info. Sols., Inc.</i> ,	
12	No. 18-CV-60178, 2018 WL 3360754 (S.D. Fla. June 29, 2018)	19
13	<i>Spokeo, Inc. v. Robins</i> ,	
14	578 U.S. 330 (2016)	20
15	<i>St. Paul Mercury Ins. Co. v. Tessler, Inc.</i> ,	
16	No. 12-cv-01827-RMW, 2016 WL 4719275 (N.D. Cal. Sept. 9, 2016)	16
17	<i>Takeya USA Corp. v. PowerPlay Mktg. Grp., LLC</i> ,	
18	No. 8:21-cv-00835-JVS, 2022 WL 17357781 (C.D. Cal. Sept. 1, 2022)	11, 12, 13
19	<i>Thomas v. Facebook, Inc.</i> ,	
20	No. 1:18-cv-00856-LJO-BAM, 2018 WL 3915585 (E.D. Cal. Aug. 15, 2018)	7
21	<i>Thornley v. Clearview AI, Inc.</i> ,	
22	984 F.3d 1241 (7th Cir. 2021)	21
23	<i>TransCore, LP v. Elec. Transaction Consultants Corp.</i> ,	
24	563 F.3d 1271 (Fed. Cir. 2009)	16
25	<i>Vance v. Microsoft Corp.</i> ,	
26	534 F. Supp. 3d 1301 (W.D. Wash. 2021)	21, 22
27	<i>Ventura v. 1st Fin. Bank USA</i> ,	
28	No. C 03-4515 JF (RS), 2005 WL 2406029 (N.D. Cal. Sept. 29, 2005)	13
	<i>Wash. Mut. Bank, FA v. Super. Ct.</i> ,	
	24 Cal. 4th 906 (2001)	8
	<i>We Are the People, Inc. v. Facebook, Inc.</i> ,	
	No. 19-cv-8871 (JMF), 2020 WL 2908260 (S.D.N.Y. June 3, 2020)	7
	<i>Zellmer v. Facebook, Inc.</i> ,	
	No. 3:18-cv-1880, 2022 WL 16924098 (N.D. Cal. Nov. 14, 2022)	20
	<i>Zinser v. Accufix Research Inst., Inc.</i> ,	
	253 F.3d 1180 (9th Cir. 2001)	8

Statutes

Cal. Civ. Code § 1798.100	9, 10, 12
Cal. Civ. Code § 1798.105	10
Cal. Civ. Code § 1798.121	10
Cal. Civ. Code § 1798.130(c)	17
Cal. Civ. Code § 1798.140(c)	11, 17
Cal. Civ. Code § 1798.140(ae)(2)(A)	11, 17
Cal. Civ. Code § 1798.150	10
Cal. Civ. Code § 1798.155	10
Cal. Civ. Code § 1798.175	11

Rules

Fed. R. Civ. P. 12(b)(6)	6, 13, 14, 17, 20
--------------------------------	-------------------

Other Authorities

Black's Law Dictionary (10th ed. 2014)	3
Black's Law Dictionary (11th ed. 2019)	14
<i>Managing a Patent</i> , U.S. Patent & Trademark Office, https://www.uspto.gov/patents/basics/manage (last visited Oct. 24, 2023)	16
<i>Proposition 24, The California Privacy Rights Act of 2020</i> , Gen. Elec. (Nov. 3, 2020), https://tinyurl.com/28mt4yxp (last visited Oct. 24, 2023)	10, 13
Public Access Opinion No. 17-011, 2017 WL 10084298 (Ill. A.G. Aug. 14, 2017)	1, 3, 14
Restatement (Second) of Conflict of Laws § 187(2)(a)–(b)	8
<i>SB-1189 Biometric Information</i> , California Legislative Information, https://tinyurl.com/mu6up6fy (last visited Oct. 24, 2023)	10

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiff Natalie Turck is an Illinois resident who claims to have used features on Meta’s Facebook and Messenger services that allowed her to input recordings of her voice for the purpose of dictating text messages, sending audio messages, and making audio calls. She claims that Meta used her voice recordings to create a *voiceprint*—which is different from a voice recording—without her consent, in violation of the Illinois Biometric Information Privacy Act (“BIPA”). Unlike a voice recording, a voiceprint is an analytical measurement of a voice’s unique qualities that can be used to identify the speaker. Ms. Turck’s entire complaint rests on unfounded and implausible speculation that when Meta collects voice recordings, it then creates voiceprints. The case should be dismissed with prejudice for several reasons.

First, and most fundamentally, Ms. Turck cannot bring claims against Meta under Illinois law. As a condition of using the Meta applications at issue, Ms. Turck agreed to resolve any disputes with Meta under California law. The binding choice-of-law provision in Meta’s terms of service precludes Ms. Turck’s Illinois claims. California has a strong interest in applying its law to any disputes over Meta’s alleged collection of biometric data, such as voiceprints. Enforcing the California choice-of-law provision requires dismissing Ms. Turck’s Illinois BIPA claims with prejudice.

Second, even if she could bring an Illinois BIPA claim, Ms. Turck fails to allege facts that would make her speculation about Meta’s conduct plausible. The complaint’s allegations focus on voice *recordings*, which are irrelevant as a matter of law because BIPA regulates *voiceprints*. Under BIPA, a voiceprint is a “distinctive pattern of curved lines and whorls made by a machine that measures human vocal sounds for the purpose of identifying an individual speaker,” and is therefore “not the same as a simple recording of a voice.” Public Access Opinion No. 17-011, 2017 WL 10084298, at *3 (Ill. A.G. Aug. 14, 2017). BIPA does not require notice, written consent, or secure storage protocols for voice recordings—only for voiceprints. The complaint’s references to Meta’s collection of voice recordings are irrelevant, because they merely describe activity that BIPA does not regulate.

When Ms. Turck does attempt to bridge the gap between voice recordings and voiceprints, she relies on two documents that fail to support her claims. The principal document Ms. Turck relies on is

1 a patent (and its continuations) that she says shows Meta theoretically could create voiceprints from
2 audio recordings collected from a hypothetical social networking system to identify users and send
3 them personalized ads. But a patent is merely a legal right to exclude others from practicing the claimed
4 invention; the existence of a patent says nothing about whether the owner actually practices the
5 invention. Thus, Ms. Turck’s allegations about the patents cannot support her claim that Meta is in
6 fact collecting voiceprints. Equally unavailing is her reliance on an out-of-context quote from a
7 regional privacy notice that Meta publishes for five states—none of which is Illinois—including
8 California, which requires companies to disclose (as Meta’s notice does) the collection of *voice*
9 *recordings* from which identifying data theoretically could be created. This notice also does not
10 support the assertion that Meta is collecting voiceprints—if anything, it shows that Meta provides the
11 required notice when state law regulates the information collected by its applications. Taken separately
12 or together, these documents suggest only what might be *possible*, and as a matter of law, alleging a
13 sheer *possibility* of misconduct is not enough to survive a motion to dismiss.

14 Further, even if the Court were to indulge Ms. Turck’s speculation that Meta collects
15 voiceprints, she alleges no facts supporting a plausible inference that Meta collected *her* voiceprint.
16 Ms. Turck alleges only that she input her voice recording into Facebook and Messenger; she then
17 asserts, in conclusory fashion, that Meta captured her individual voiceprint. But she alleges no facts to
18 substantiate that conclusion. Meta’s patent refers to a hypothetical “social networking system,” and
19 the regional privacy notice applies to more than a dozen of Meta’s services. Nothing in these sources
20 suggests that Meta collects voiceprints from *Facebook or Messenger*. Ms. Turck’s threadbare
21 allegation that Meta collects audio from third-party sources and uses that audio to create voiceprints
22 for people is even further afield, because Ms. Turck cannot plausibly allege that *her* voice recording
23 was in such audio, much less that Meta created *her* voiceprint from *that* audio. Ms. Turck piles
24 speculation on speculation, and none of it is even specific to her.

25 The complaint’s many pages devoted to Meta’s privacy disclosures do nothing to support these
26 claims. Ms. Turck alleges that Meta does not disclose that it collects voiceprints, and she concludes
27 that Meta has violated BIPA. But she alleges no facts tending to exclude the obvious alternative
28 inference—that Meta’s disclosures are lawful because Meta does not collect voiceprints.

1 *Finally*, Ms. Turck independently fails to state claims under BIPA based on Meta supposedly
 2 profiting from voiceprints and failing to store voiceprints securely. She alleges nothing that could
 3 constitute a “profit” under BIPA, and no factual basis for her speculation that Meta does not securely
 4 store any voiceprints it supposedly collects. The complaint should be dismissed with prejudice.

5 **II. FACTUAL BACKGROUND**

6 **A. The Illinois Biometric Information Privacy Act**

7 The Illinois Legislature enacted BIPA in 2008 in response to the growing use of biometric
 8 identification technologies “in the business and security screening sectors” in Illinois. 740 Ill. Comp.
 9 Stat. 14/5(a). BIPA regulates the use of “biometric identifiers,” defined as six specific types of data
 10 used for biometric identification: fingerprints, voiceprints, retina scans, iris scans, scans of hand
 11 geometry, and scans of face geometry. *Id.* at 14/10. BIPA does not define “voiceprint,” but the Illinois
 12 Attorney General has adopted the term’s plain meaning, explaining that a voiceprint is “not the same
 13 as a simple recording of a voice.” Public Access Opinion No. 17-011, 2017 WL 10084298, at *3.
 14 Rather, a voiceprint is a “distinctive pattern of curved lines and whorls made by a machine that
 15 measures human vocal sounds for the purpose of identifying an individual speaker.” *Id.* (quoting
 16 Black’s Law Dictionary (10th ed. 2014)).

17 To complement this regulation, the statute also regulates the use of derivative data called
 18 “biometric information,” defined as any information “based on an individual’s biometric identifier”—
 19 “regardless of how it is captured, converted, stored, or shared”—that is “used to identify an individual.”
 20 740 Ill. Comp. Stat. 14/10. In other words, the Illinois legislature sought to ensure that “whatever [one]
 21 does in manipulating a biometric identifier . . . , the resulting information is still covered” by BIPA if
 22 it can still “be used to identify the person.” *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1095 (N.D.
 23 Ill. 2017).

24 BIPA imposes certain requirements on private entities that collect or possess biometric
 25 identifiers and biometric information (together, “biometric data”). Under Section 15(a), an entity that
 26 possesses biometric data must make available to the public and comply with a written policy governing
 27 the retention and deletion of such data. 740 Ill. Comp. Stat. 14/15(a). Under Section 15(b), an entity
 28 that collects a person’s biometric data must first provide notice to and obtain consent from that person.

Id. at 14/15(b). Under Section 15(c), an entity that possesses biometric data may not “sell, lease, trade, or otherwise profit from” the data. *Id.* at 14/15(c). And under Section 15(e), an entity that possesses biometric data must “store, transmit, and protect [the data] from disclosure . . . using the reasonable standard of care within” that entity’s industry and in the same or a more protective manner than it “stores, transmits, and protects other confidential and sensitive information.” *Id.* at 14/15(e).

BIPA provides a private right of action for “[a]ny person aggrieved by a violation” to recover the greater of “\$1,000 or actual damages” per negligent violation, and the greater of “\$5,000 or actual damages” per reckless or intentional violation. 740 Ill. Comp. Stat. 14/20.

B. Meta’s Facebook And Messenger Services

Meta is a technology company that offers a number of applications that connect people, communities, and businesses. One such application—Facebook—is an online service that allows users to connect with friends, family, and communities who share their interests. Compl. ¶ 2. Messenger is a feature on Facebook that allows Facebook users to communicate with other Facebook users by sharing instant messages, photos, videos, and audio recordings, or by connecting in real time through an audio or video call. *Id.* ¶ 3.

Together, Facebook and Messenger offer various features that allow users to record or transmit their voices. For example, Facebook users can use Messenger’s voice-to-text dictation feature to dictate messages into their devices and convert them into text messages to send to other Facebook users. Compl. ¶ 75. Users also can “send an audio recording via Messenger, make calls via Messenger,” or provide audio through Facebook, such as by “dictating a Facebook search, inputting their name pronunciation, posting an audio file, or posting a video that includes audio.” *Id.* ¶ 76.

C. Meta’s Privacy Policies

All Facebook users agree to Meta’s privacy policies, which are also posted on its website. These policies disclose the information Meta collects about its users and how it uses and shares that information. Compl. ¶ 98; *see* RJN, Ex. A–B.¹ Meta’s Privacy Policy covers Facebook and Messenger

¹ By separate motion, Meta moves for incorporation by reference or judicial notice of Meta’s Privacy Policy, Regional Privacy Notice, current and former Terms of Service, and Facebook sign-up page because the complaint relies on these documents, either explicitly or implicitly. Meta cites these documents only for background or to establish the applicable law governing Ms. Turck’s claims. As explained further in Meta’s separate motion, although this Court denied Meta’s request for judicial

(among other services) and describes the information Meta collects from users. Compl. ¶¶ 117–18; RJN, Ex. A at 3–10. For example, Meta discloses to users that if they provide content on Meta’s services using “voice-enabled features,” Meta may use that content to enable users “to make voice and video calls and connect with others.” Compl. ¶ 120; RJN, Ex. A at 82.

Meta’s United States Regional Privacy Notice supplements the Privacy Policy for people who use Facebook and Messenger (among other services) and live in the United States. Compl. ¶ 131; *see* RJN, Ex. B. Similar to the Privacy Policy, this notice explains to users “how [Meta] collect[s], use[s], and disclose[s]” their personal information. Compl. ¶ 133; RJN, Ex. B at 1. But the Regional Privacy Notice also specifically describes how users in the United States may exercise their rights under the privacy laws of five states: California, Colorado, Connecticut, Utah, and Virginia. Compl. ¶ 133; RJN, Ex. B at 1. Illinois is not included. The Regional Privacy Notice discloses that, depending on how users interact with its services, Meta “may” collect their “sensitive personal information” as defined by those five states’ privacy laws, including “voice recordings which may be used to identify you.” Compl. ¶ 141; RJN, Ex. B at 4.

D. Ms. Turck’s Claims

Ms. Turck is an Illinois citizen who has a Facebook account and uses Messenger. Compl. ¶¶ 25, 148. She alleges that “[o]n multiple occasions” in 2022 and 2023, she “input her voice into an audio function on Facebook or Messenger” to perform certain tasks, including “to dictate text messages to send via Messenger, sen[d] an audio recording of her voice via Messenger, and mak[e] audio calls via Messenger.” *Id.* ¶ 149. Ms. Turck also alleges, “[u]pon information and belief,” that Meta received audio recordings not just through Facebook or Messenger, but also from “[c]ompanies or organizations” that do not use Meta’s services but provide Meta with audio content, *id.* ¶¶ 77, 81, 117, 124–25, and that she “believes that . . . her voice has been captured by Meta . . . via [such] third parties,” *id.* ¶ 150. Ms. Turck asserts that Meta not only collected these recordings of her voice, but that it used them to collect her “voiceprint and related biometric information.” *Id.* ¶¶ 151–52. Ms. Turck alleges that, in connection with that collection of voiceprints, Meta violated BIPA Sections 15(a),

notice in *Gershzon v. Meta Platforms, Inc.*, No. 23-cv-00083-SI, 2023 WL 5420234, at *9 n.3 (N.D. Cal. Aug. 22, 2023), *Gershzon* is distinguishable because here, the Court need not draw factual inferences from the cited documents.

15(b), 15(c), and 15(e). *Id.* ¶¶ 165–202. She seeks to represent a class of all “natural persons in Illinois from whom Meta created, collected, captured, received, obtained, or stored” a voiceprint. *Id.* ¶ 153.

III. LEGAL STANDARD

For her complaint to survive a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), Ms. Turck must “plead[] factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). This requires more than “a sheer possibility that a defendant has acted unlawfully,” *id.*, and “must be enough to raise a right to relief above the speculative level,” *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007). The pleading must include “facts tending to exclude the possibility that the alternative explanation is true.” *In re Century Aluminum Co. Sec. Litig.*, 729 F.3d 1104, 1108 (9th Cir. 2013). In other words, “[w]here a complaint pleads facts that are ‘merely consistent with’ a defendant’s liability, it ‘stops short of the line between possibility and plausibility of entitlement to relief.’” *Iqbal*, 556 U.S. at 678. A plaintiff “armed with nothing more than conclusions” instead of well-pleaded factual allegations is not entitled to “unlock the doors of discovery.” *Id.* at 678–79.

IV. ARGUMENT

A. The BIPA Claims Are Barred By The California Choice-Of-Law Clause To Which Ms. Turck Agreed In Meta’s Terms Of Service

1. Ms. Turck Is Bound By The California Choice-Of-Law Clause In Meta’s Terms Of Service

Ms. Turck alleges that she “has a Facebook account and utilizes Meta’s Messenger app,” and that she has used these accounts in 2022 and 2023. Compl. ¶¶ 148–49. She does not allege when she first signed up for her Facebook account. But regardless of when Ms. Turck signed up for her Facebook Account, she agreed to be bound by Meta’s Terms of Service as a condition of her use of Facebook and Messenger. *See* RJN, Ex. F (notifying users that “By clicking Sign Up, you agree to our Terms [of Service]”).

Additionally, because Ms. Turck alleges that she used Facebook and Messenger in 2022 and 2023, she would have agreed to Meta’s current Terms of Service as a condition of her continued use. When Meta updates its Terms of Service, it notifies users of its changes and explains that if they continue to use Facebook or Messenger, they will be bound to the updated terms. RJN, Ex. C at 9;

1 *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1177 (9th Cir. 2014) (recognizing that courts enforce
 2 agreements “where the website contains an explicit textual notice that continued use will act as a
 3 manifestation of the user’s intent to be bound”). Meta’s Terms of Service were last updated on July
 4 26, 2022, RJN, Ex. C at 13, and thus were in effect when Ms. Turck alleges that she used Facebook
 5 and Messenger.²

6 Courts across the country have repeatedly enforced Meta’s Terms of Service.³ At all relevant
 7 times, including in 2022 and 2023, those terms have contained a California choice-of-law clause. RJN,
 8 Ex. C at 10–11, Ex. D at 9, Ex. E at 9. Under that provision, the parties agreed that “the laws of the
 9 State of California will govern . . . any claim, cause of action, or dispute” between Meta and Ms. Turck
 10 that “arises out of or relates to . . . [her] access or use of” Facebook and Messenger. *Id.* Ms. Turck
 11 claims that Meta violated BIPA by obtaining her “voiceprint and related biometric information” from
 12 audio she input “into . . . Facebook or Messenger.” Compl. ¶¶ 148–52. Thus, her claims arise directly
 13 from her use of those applications and are covered by the plain text of the choice-of-law provision.
 14 The only question remaining is whether applicable choice-of-law rules provide a basis for declining to
 15 enforce the parties’ agreement. As explained below, they do not.

16
 17
 18
 19 ² Ms. Turck does not allege what months or days she used Facebook or Messenger in 2022 and 2023,
 20 but the current Terms of Service would apply to her when using either application after they took effect
 21 on July 26, 2022. To the extent Ms. Turck used Facebook or Messenger in the first seven months of
 22 2022, she would have been bound by a prior version of Meta’s Terms of Service, which contained an
 23 identical choice-of-law-clause. RJN, Ex. D at 9, Ex. E at 9.

24 ³ See *Davis v. Meta Platforms, Inc.*, No. 4:22-cv-01001, 2023 WL 4670491, at *10 (E.D. Tex. July 20,
 25 2023) (holding that Meta’s Terms of Service and the dispute resolution section within are valid and
 26 enforceable); *Loveland v. Facebook*, No. 20-cv-6260-JMY, 2021 WL 1734800, at *5 (E.D. Pa. May 3,
 27 2021) (same); *We Are the People, Inc. v. Facebook, Inc.*, No. 19-cv-8871 (JMF), 2020 WL 2908260,
 28 at *2 (S.D.N.Y. June 3, 2020) (same); *Loomer v. Facebook, Inc.*, No. 19-cv-80893, 2020 WL 2926357,
 at *3 (S.D. Fla. Apr. 13, 2020) (same); *Hayes v. Facebook*, No. 18-cv-02333-MEH, 2019 WL 8275335,
 at *2–3 (D. Colo. Mar. 6, 2019) (same); *Fteja v. Facebook, Inc.*, 841 F. Supp. 2d 829, 841 (S.D.N.Y.
 2012) (same); *Miller v. Facebook, Inc.*, No. 1:09-cv-2810-RLV, 2010 WL 9525523, at *3 (N.D. Ga.
 Jan. 15, 2010) (same); *cf. Thomas v. Facebook, Inc.*, No. 1:18-cv-00856-LJO-BAM, 2018 WL
 3915585, at *4 (E.D. Cal. Aug. 15, 2018) (enforcing Facebook’s Terms of Service, formerly known as
 the Statement of Rights and Responsibilities, and observing that “[n]umerous courts have affirmed the
 validity and enforceability of Facebook’s [Terms]”); *Dolin v. Facebook, Inc.*, 289 F. Supp. 3d 1153,
 1160 (D. Haw. 2018) (similar).

2. The California Choice-Of-Law Clause Bars Ms. Turck's Claims Under BIPA

When assessing a choice-of-law clause, “[a] federal court sitting in diversity must look to the forum state’s choice-of-law rules.” *In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 447 (N.D. Cal. 2018) (quoting *Zinser v. Accufix Research Inst., Inc.*, 253 F.3d 1180, 1187 (9th Cir. 2001)). “Where, as here, the parties have entered an agreement containing a choice of law provision,” *Frenzel v. Aliphcom*, No. 14-cv-03587-WHO, 2015 WL 4110811, at *6 (N.D. Cal. July 7, 2015), California courts follow Section 187(2)(b) of the Restatement (Second) of Conflict of Laws, which “reflects a strong policy favoring enforcement of such provisions,” *Nedlloyd Lines B.V. v. Super. Ct.*, 3 Cal. 4th 459, 465 (1992); *see also Wash. Mut. Bank, FA v. Super. Ct.*, 24 Cal. 4th 906, 917 (2001) (holding that *Nedlloyd*’s analysis applies to consumer contracts).

The Court must apply the “law of the state chosen by the parties”—here, California—unless one of two narrow exceptions applies: (1) California “has no substantial relationship to the parties or the transaction and there is no other reasonable basis for the parties’ choice”; or (2) applying California law “would be contrary to a fundamental policy of a state which has a materially greater interest than the chosen state in the determination of the particular issue and which . . . would be the state of the applicable law in the absence of an effective choice of law by the parties.” *Nedlloyd*, 3 Cal. 4th at 465 (quoting Restatement (Second) of Conflict of Laws § 187(2)(a)–(b)).

Meta “bears the burden to establish a sufficient relationship to” California, as the parties’ chosen state law. *LeBoeuf v. NVIDIA Corp.*, No. 19-cv-03543-SVK, 2019 WL 13210428, at *6 (N.D. Cal. Nov. 18, 2019) (quoting *Colaco v. Cavotec SA*, 25 Cal. App. 5th 1172, 1188 (2018)). Once that is established, the burden shifts to Ms. Turck to establish both (a) “a fundamental conflict in the states’ laws” and (b) that Illinois has a materially greater interest than California in the determination of Ms. Turck’s claims. *Id.*

As to the first exception, “[i]f one of the parties resides in the chosen state,” the parties have a substantial relationship to the state and “a reasonable basis for their choice.” *Nedlloyd*, 3 Cal. 4th at 467. Meta’s principal place of business is in California. Compl. ¶¶ 28–29. That alone “satisfies this inquiry.” *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1168 (N.D. Cal. 2016); *Palomino v. Facebook, Inc.*, No. 16-cv-04230-HSG, 2017 WL 76901, at *3 (N.D. Cal. Jan. 9, 2017)

1 (“California has a substantial relationship to the parties because ‘Defendant is headquartered in
2 California and maintains its principal place of business in California.’”).

3 Ms. Turck thus bears the burden of demonstrating that the second exception is satisfied. The
4 first question is whether California law “is contrary to a fundamental policy of [Illinois].” *Nedlloyd*, 3
5 Cal. 4th at 466 (emphasis omitted). In other words, if California’s and Illinois’ laws regulating the
6 privacy of consumers’ biometric data do not fundamentally conflict, the Court “shall enforce the
7 parties’ choice of law.” *Id.* But if the Court determines that there is a fundamental conflict, it “must
8 then determine whether [Illinois] has a ‘materially greater interest than [California]’” in the outcome
9 of this case. *Id.* If not, the Court should enforce the choice-of-law provision. *Id.* Here, applying
10 California law would not be contrary to any fundamental public policy in Illinois because the two
11 states’ biometric data privacy laws do not fundamentally conflict. And, even if applying California
12 law here would be contrary to Illinois law, Illinois does not have a materially greater interest than
13 California in the resolution of Ms. Turck’s claims.

14 **a. California’s Biometric Data Privacy Law Does Not Fundamentally**
15 **Conflict With Illinois Public Policy**

16 Assuming *arguendo* that Ms. Turck can satisfy her burden to show that BIPA reflects Illinois’
17 fundamental public policy, *LeBoeuf*, 2019 WL 13210428, at *6, BIPA does not fundamentally conflict
18 with California’s law regulating the use of biometric data because California provides comparable—if
19 not greater—protections to consumers. *See Brazil v. Dell Inc.*, 585 F. Supp. 2d 1158, 1165–66 (N.D.
20 Cal. 2008) (refusing to recognize a fundamental conflict where Texas law “provides comparable
21 protection [as California law] under the facts of this case”).

22 California enacted the California Consumer Privacy Act (“CCPA”) in 2018 and the California
23 Privacy Rights Act (“CPRA”) in 2020 (effective 2023), which amended and restated the CCPA. The
24 CCPA comprehensively regulates the collection and use of consumers’ biometric data. Among other
25 things, the CCPA requires businesses to inform consumers of (1) the collection of their biometric data
26 (at or before the point of collection); (2) the purposes for which their biometric data will be collected
27 or used; (3) whether their biometric data will be disclosed; and (4) the business’s retention policy for
28 the biometric data. Cal. Civ. Code § 1798.100. Consumers have the right to limit how businesses may

1 use or disclose their biometric data. *Id.* § 1798.121. Consumers also may request that businesses delete
 2 their biometric data and other personal information. *Id.* § 1798.105. The California Attorney General
 3 is authorized to enforce these requirements and may seek statutory penalties of up to \$7,500 per
 4 intentional violation of the statute and up to \$2,500 per non-intentional violation. *Id.* § 1798.155.
 5 Consumers have a private right of action to recover statutory damages up to \$750 or their actual
 6 damages, whichever is greater, for violations of the CCPA in the event of a data breach. *Id.*
 7 § 1798.150.⁴

8 The CCPA imposes requirements similar to BIPA's: Both regimes require businesses that
 9 collect or use consumers' biometric data to disclose how their data will be collected and used and for
 10 how long it will be retained. *Compare* Cal. Civ. Code § 1798.100, *with* 740 Ill. Comp. Stat. 14/15(a).
 11 And both regimes provide consumers with control over whether businesses collect their biometric data
 12 at all. BIPA provides that businesses must obtain a written release from consumers before collecting
 13 their biometric data, 740 Ill. Comp. Stat. 14/15(b)(3), while the CCPA allows consumers to direct
 14 businesses not to use or disclose their biometric data and other sensitive personal information for
 15 certain purposes and to request that they delete such information, Cal. Civ. Code §§ 1798.105,
 16 1798.121. Additionally, both regimes were enacted with the goal of strengthening consumers' privacy
 17 rights, while also recognizing that there are benefits to allowing businesses to use biometric data.
 18 *Compare* 740 Ill. Comp. Stat. 14/5 (explaining that "[t]he use of biometrics . . . appears to promise
 19 streamlined financial transactions and security screenings," and that regulating businesses' use of such
 20 data would encourage consumer trust in and adoption of biometric systems), *with Proposition 24, The*
 21 *California Privacy Rights Act of 2020*, Gen. Elec. (Nov. 3, 2020), <https://tinyurl.com/28mt4yxp> (last
 22 visited Oct. 24, 2023) (noting the goal of amending the CCPA is to "strengthen[] consumer privacy
 23

24
 25 ⁴ The CCPA reflects California's public policy of allowing consumers to seek redress for actual harm
 26 from statutory violations, while reserving to the State the power to seek penalties for technical
 27 violations that caused no harm. The California legislature considered—and rejected—a proposed
 28 amendment to the CPRA (amending the CCPA) modeled after BIPA that would have allowed
 consumers to recover statutory damages for biometric privacy violations in the absence of an actual,
 real-world injury. *See SB-1189 Biometric Information*, California Legislative Information,
<https://tinyurl.com/mu6up6fy> (last visited Oct. 24, 2023). Consumers who experience actual concrete
 harm may still sue for statutory or actual damages. Cal. Civ. Code § 1798.150.

1 while giving attention to the impact on business and innovation”); Cal. Civ. Code § 1798.175 (CCPA
2 was enacted to “further the constitutional right of privacy”).

3 When it comes to the use of a person’s voice, California provides *greater* protection to
4 consumers than Illinois does. The CCPA regulates businesses’ collection and use of mere “voice
5 recordings, from which an identifier template, such as a . . . voiceprint, *can* be extracted.” Cal. Civ.
6 Code § 1798.140(c), (ae)(2)(A) (emphasis added). BIPA does not regulate the collection and use of
7 mere voice recordings; it regulates only the collection and use of “voiceprints”—unique identifier
8 templates that *have* been extracted from voice recordings. 740 Ill. Comp. Stat. 14/10. Because there
9 are no “substantive differences between [Illinois] and California law that would offend” Illinois’ public
10 policy, there is no fundamental conflict warranting displacing the parties’ choice of California law.
11 *Rojas-Lozano v. Google, Inc.*, 159 F. Supp. 3d 1101, 1112 (N.D. Cal. 2016); *see also Palomino*, 2017
12 WL 76901, at *4 (holding no fundamental conflict existed between New Jersey and California
13 consumer protection law because California “has its own robust body of consumer protection law” that
14 provided equal or greater protections to consumers than New Jersey).

15 Although a court in this district held seven years ago that California law conflicted with Illinois’
16 fundamental public policy of protecting the privacy of consumers’ biometric data, *see Facebook*
17 *Biometric*, 185 F. Supp. 3d at 1169–70, California’s laws regulating biometric data have fundamentally
18 changed since that decision. In that case, the plaintiffs alleged that Meta (then known as “Facebook”)
19 violated BIPA by creating and storing facial-recognition templates for Facebook users without their
20 consent. *Id.* at 1158–59. Meta argued that California law applied to the dispute pursuant to the choice-
21 of-law clause in Meta’s Terms of Service. *Id.* at 1158. After holding an evidentiary hearing, the court
22 ruled that the plaintiffs’ assent to Meta’s Terms of Service as a condition of signing up for Facebook
23 constituted a valid agreement to resolve disputes under California law. *Id.* at 1164–67. However, the
24 court declined to enforce the choice-of-law clause because, in its view, applying California law as it
25 existed at that time would offend Illinois’ fundamental public policy reflected by BIPA. *Id.* at 1170.
26 In so holding, the court opined that “California ha[d] no law or policy equivalent to BIPA,” and
27 applying California law would therefore “writ[e] out of existence” the “Illinois policy of protecting its
28 citizens’ privacy interests in their biometric data.” *Id.* at 1169. *But see Takeya USA Corp. v. PowerPlay*

1 *Mktg. Grp., LLC*, No. 8:21-cv-00835-JVS (DFMx), 2022 WL 17357781, at *8 (C.D. Cal. Sept. 1, 2022)
 2 (“California courts have . . . declined to find a fundamental conflict even where a state has greater
 3 protections than the chosen state.”).

4 The subsequent enactment of the CCPA vitiates the core premise of the *Facebook Biometric*
 5 ruling: It is no longer true that “California has no law or policy equivalent to BIPA.” 185 F. Supp. 3d
 6 at 1169. To the extent that “BIPA manifests Illinois’ substantial policy of protecting its citizens’ right
 7 to privacy in their personal biometric data,” the CCPA now does the same in California. *Id.*; *see also*
 8 Cal. Civ. Code § 1798.100 *et seq.* Because California’s protections for consumers are comparable to
 9 Illinois’ protections, and the differences between the statutes do not amount to a fundamental conflict,
 10 applying California law to Ms. Turck’s biometric privacy claims would not be contrary to any
 11 fundamental policy of Illinois.

12 **b. Illinois Does Not Have A Materially Greater Interest In The Outcome Of**
 13 **This Case**

14 Even if there were a fundamental conflict between California’s and Illinois’ laws regulating
 15 biometric data, it would still be proper to enforce the parties’ choice of California law: California has
 16 at least an equal interest in applying its laws here. “In determining which state has a materially greater
 17 interest, California courts consider which state, in the circumstances presented, will suffer greater
 18 impairment of its policies if the other state’s law is applied.” *MaxLite, Inc. v. ATG Electronics, Inc.*,
 19 No. 8:20-cv-01056-MCS-ADS, 2022 WL 16923391, at *7 (C.D. Cal. Aug. 7, 2022). If the chosen
 20 state has at least an equal interest in the matter, the Court should enforce the choice-of-law provision.
 21 *See Takeya*, 2022 WL 17357781, at *11.

22 Although Ms. Turck is a citizen of Illinois, Compl. ¶ 25, Meta is a citizen of California, *id.* ¶ 26,
 23 and the complaint does not allege that Meta engaged in any conduct in Illinois or specifically targeting
 24 Illinois residents. California has at least an equally compelling interest as Illinois in applying its laws
 25 regulating companies’ use of biometric data and enforcing its policy to address technical violations
 26 under the CCPA through actions brought by the state Attorney General. California’s citizens voted to
 27 approve the CPRA (amending the CCPA) with the specific “goal of strengthening consumer privacy
 28 while giving attention to the impact on business and innovation,” in recognition that “California is the

world leader in many new technologies that have reshaped our society.” *Proposition 24, The California Privacy Rights Act of 2020*, Gen. Elec. (Nov. 3, 2020), <https://tinyurl.com/28mt4yxp> (last visited Oct. 24, 2023); *see also Ventura v. 1st Fin. Bank USA*, No. C 03-4515 JF (RS), 2005 WL 2406029, at *5 (N.D. Cal. Sept. 29, 2005) (holding that although “California has an interest in protecting the rights of its resident,” South Dakota—the parties’ chosen state law—“has an equal interest in protecting the rights of its resident businesses”).

Additionally, applying California law is consistent with the parties’ expectations. In the same provision of the Terms of Service containing the choice-of-law clause, the parties also agreed to resolve any disputes between them “exclusively in the U.S. District Court for the Northern District of California” or in state court in San Mateo County. RJN, Ex. C at 11, Ex. D at 9, Ex. E at 9. The fact that Ms. Turck filed suit in the agreed California forum suggests that she understands the parties’ agreement about where and how their disputes would be resolved. Enforcing the California choice-of-law clause would therefore align “with the parties’ expectations.” *Takeya*, 2022 WL 17357781, at *10.

Thus, the Court should enforce the parties’ agreement to apply California law to Ms. Turck’s claims. *Nedlloyd*, 3 Cal. 4th at 465. Under that agreement, Ms. Turck cannot bring BIPA claims against Meta, and the Court should dismiss her complaint with prejudice.

B. Even If Illinois Law Applies, Ms. Turck’s BIPA Claims Fail Because They Are Conclusory And Speculative

If the Court declines to enforce the parties’ choice-of-law clause, the Court nevertheless should dismiss Ms. Turck’s complaint in full because she fails to plead facts that make her BIPA claims plausible. All of the claims fail because Ms. Turck has not plausibly alleged, and cannot plausibly allege, that Meta collects voiceprints. Even if the Court accepted the assumption that Meta collects voiceprints, Ms. Turck has not plausibly alleged that Meta collects voiceprints from anyone who uses Facebook and Messenger, much less her own voiceprint.

At most, Ms. Turck has alleged that it is theoretically possible that Meta collected her voiceprint without providing the required disclosures under BIPA. But the Ninth Circuit has repeatedly recognized that such allegations are insufficient to state a claim under Rule 12(b)(6). *See Century Aluminum*, 729 F.3d at 1108; *Gonzalez v. Planned Parenthood of L.A.*, 759 F.3d 1112, 1116 (9th Cir.

2014) (affirming dismissal of the plaintiff’s claims because her allegations suggested only that the defendant’s conduct was “merely *possible* rather than plausible” (emphasis in original)). Further, Ms. Turck’s allegations are insufficient to state a claim under Rule 12(b)(6) because they do not tend to exclude the possibility that the alternative inference—that Meta did not collect voiceprints—is true. *Century Aluminum*, 729 F.3d at 1108; *see also Eclectic Props. E., LLC v. Marcus & Millichap Co.*, 751 F.3d 990, 998, 1000 (9th Cir. 2014) (affirming dismissal of fraud claims because the plaintiff’s allegations did “not tend to exclude a plausible and innocuous alternative explanation”); *A.C.L. Computers & Software, Inc. v. United States*, 727 F. App’x 376, 376 (9th Cir. 2018) (holding the plaintiff did not plausibly plead a conversion claim because there were “multiple explanations for the loss” of its merchandise that did not involve the defendants “aiding in the theft of shipments”).

1. Plaintiff Does Not Plausibly Allege That Meta Collects Voiceprints From Anyone

Ms. Turck alleges that she used features on Facebook and Messenger that “collect audio of users’ voices.” Compl. ¶¶ 75, 149; *see also, e.g., id.* ¶¶ 76–79. Specifically, she alleges that she used voice-to-text features, made audio calls, and sent voice messages. *Id.* ¶ 149. But BIPA does not regulate the collection of audio recordings. Instead, it regulates the collection and possession of “voiceprint[s].” 740 Ill. Comp. Stat. 14/10. A “voiceprint” under BIPA is *more* than a mere “recording of a voice.” Public Access Opinion No. 17-011, 2017 WL 10084298, at *3; *Rivera*, 238 F. Supp. 3d at 1097 (explaining BIPA does not apply if an entity “records a person’s voice without generating a voiceprint”); *see also McGoveran v. Amazon Web Servs., Inc.*, No. 1:20-cv-01399-SB, 2023 WL 2683553, at *10 (D. Del. Mar. 29, 2023) (dismissing BIPA claim where plaintiff alleged the use of “their voice audio” because “under [BIPA], voice audio alone is” not a “voiceprint”). Instead, a “voiceprint” is data derived from a voice recording that identifies a person. Specifically, a voiceprint is a “distinctive pattern of curved lines and whorls made by a machine that measures human vocal sounds for the purpose of identifying an individual speaker.” *Carpenter v. McDonald’s Corp.*, 580 F. Supp. 3d 512, 515 (N.D. Ill. 2022) (quoting Black’s Law Dictionary (11th ed. 2019)); *accord* Public Access Opinion No. 17-011, 2017 WL 10084298, at *3.

Ms. Turck relies entirely on two allegations to support the leap from voice *recordings* to *voiceprints*: (1) patents that show that Meta would have intellectual property protections if it *did* create

voiceprints from audio recordings in a particular way; and (2) language in a privacy notice expressly directed at Meta’s compliance with California law, which (unlike Illinois law) requires entities to disclose when they may collect voice *recordings* from which a voiceprint theoretically could be created—i.e., any recording of a voice. At most, these two allegations suggest that Meta *could* create voiceprints. But that sheer possibility does not “allo[w] the court to draw the reasonable inference” that Meta *is* collecting voiceprints from Facebook and Messenger users without required disclosure in violation of BIPA. *Iqbal*, 556 U.S. at 678. Nor does it tend to exclude the more obvious inference: that Meta does not collect voiceprints. *Century Aluminum*, 729 F.3d at 1108.

a. Meta’s Patents Do Not Plausibly Suggest That Meta Collects Or Uses Voiceprints

Ms. Turck rests her voiceprint theory on the allegation that Meta owns a patent (and its continuations from 2020 through 2023) claiming a method of voice-recognition in a hypothetical “social networking system.” Nothing in the patents contemplate anything like what she alleges happened here. The patents make no mention of Facebook or Messenger, and they do not describe the creation of voiceprints from audio recordings collected from audio calls, voice messages, or voice-dictation features. *See* Compl. ¶¶ 52–74. Nevertheless, Ms. Turck asserts that the patents somehow support the allegation that Meta did exactly that because they contemplate a technology that creates voiceprints. *Id.*

The patents do not support the weight that Ms. Turck asks the Court to put on them: Simply alleging that Meta owns certain patents for voiceprinting technology does not suggest that those patents “could have been implemented,” much less “ha[ve] been implemented,” including in any particular way. *Casey v. Toyota Motor Eng’g & Mfg. N. Am., Inc.*, 770 F.3d 322, 334 (5th Cir. 2014). Meta owns many patents describing technology it has not implemented and might never implement in any way.⁵ “It is elementary” that a patent confers nothing more on its owner than the right to exclude others

⁵ Ms. Turck’s own allegations illustrate this: The patents contemplate a system through which Meta could target personalized TV ads to one of its users watching TV at her friend’s house by receiving her voice audio through “a dangle in communication with the TV” and then identifying her through her voiceprint. *See* Compl. ¶ 61. Although such technology might be conceivable, no one would plausibly claim—and it does not appear that Ms. Turck even claims—that Meta is targeting television ads to viewers wherever they might be.

1 from practicing a claimed invention. *See Emblaze Ltd. v. Apple Inc.*, No. 5:11-cv-01079-PSG, 2015
 2 WL 396010, at *8 (N.D. Cal. Jan. 29, 2015), *aff'd*, 639 F. App'x 639 (Fed. Cir. 2016). And “patent
 3 rights do not depend upon the exercise of [the patentee’s] rights.” *King Instruments Corp. v. Perego*,
 4 65 F.3d 941, 949 (Fed. Cir. 1995). The Supreme Court has held that an “invention” within the meaning
 5 of the Patent Act “unquestionably refers to the inventor’s *conception* rather than to a physical
 6 embodiment of that idea,” and “[t]he statute does not contain any express requirement that an invention
 7 must be reduced to *practice* before it can be patented.” *Pfaff v. Wells Elecs., Inc.*, 525 U.S. 55, 60
 8 (1998) (emphases added). Rather, “[i]t is well settled that an invention may be patented before it is
 9 reduced to practice.” *Id.* at 61 (adding that Alexander Graham Bell received a patent for the telephone
 10 “before constructing a working telephone”). As a matter of law, “[a] patent is granted in exchange for
 11 a patentee’s disclosure of an invention, *not for the patentee’s use of the invention.*” *Rite-Hite Corp. v.*
 12 *Kelley Co.*, 56 F.3d 1538, 1547 (Fed. Cir. 1995) (en banc) (emphasis added). “There is no requirement
 13 in this country that a patentee make, use, or sell its patented invention.” *Id.* Thus, holding a patent for
 14 an invention that would allow the owner to practice the technology does not mean or even imply that
 15 the owner is *actually* practicing the technology, much less that that the owner is doing so in any
 16 particular form or context. *See, e.g., TransCore, LP v. Elec. Transaction Consultants Corp.*, 563 F.3d
 17 1271, 1275 (Fed. Cir. 2009) (“[T]he grant of a patent does not provide the patentee with an affirmative
 18 right to practice the patent but merely the right to exclude.”); *St. Paul Mercury Ins. Co. v. Tessera, Inc.*,
 19 No. 12-cv-01827-RMW, 2016 WL 4719275, at *3 (N.D. Cal. Sept. 9, 2016) (same).

20 Ms. Turck’s allegations simply *assume* that Meta has made the significant effort to
 21 commercialize its patented invention, and that Meta itself practices that invention. And Ms. Turck’s
 22 allegations further *assume* that Meta does all of this in the specific manner she theorizes. These
 23 assumptions provide no plausible support for her conclusory allegation that Meta has collected her
 24 voiceprint. Owning a patent does not plausibly suggest the patentholder is engaged in any patented
 25 conduct, *especially* “if exercising the rights related to the invention would violate any law.” *Managing*
 26 *a Patent*, U.S. Patent & Trademark Office, <https://www.uspto.gov/patents/basics/manage> (last visited
 27 Oct. 24, 2023). If the Court were to hold that such allegations satisfy pleading standards under Rule
 28

1 8(a) and Rule 12(b)(6), any plaintiff could sue a patent holder for allegedly committing acts it has only
 2 the right to exclude others from practicing. That is not the law.

3 **b. Meta’s Regional Privacy Notice Does Not Suggest That Meta Collects Or**
 4 **Uses Voiceprints**

5 Ms. Turck also cites Meta’s Regional Privacy Notice to support her assertion that Meta collects
 6 voiceprints. Specifically, she points to a section of the notice in which Meta discloses certain categories
 7 of “sensitive personal information”—“*as defined in*” a list of laws in California, Colorado, Connecticut,
 8 Utah, and Virginia—that Meta may collect. Compl. ¶ 139. Those categories include, among other
 9 things, “*voice recordings* which may be used to identify you.” *Id.*; RJN, Ex. B at 4 (emphasis added).
 10 Ms. Turck asserts, in essence, that this language concedes the collection of *voiceprints* under BIPA.
 11 Compl. ¶ 92; *see also id.* ¶ 140 (asserting that the notice reveals that Meta “can use” voice audio to
 12 identify users). But the language says no such thing, and Ms. Turck’s assertion is implausible.

13 There is an obvious—and lawful—explanation for this language. California’s CCPA, one of
 14 the laws that the relevant section of the Regional Privacy Notice is expressly directed at addressing,
 15 requires businesses to disclose their collection of “voice recordings[] from which an identifier template,
 16 such as a . . . voiceprint, can be extracted”—i.e., any audio that includes a voice. Cal. Civ. Code
 17 §§ 1798.130(c), 1798.140(c), 1798.140(ae)(2)(A). The Regional Privacy Notice thus satisfies Meta’s
 18 disclosure obligation under the CCPA: Because the statute requires Meta to disclose that it collects
 19 *voice recordings that could be turned into voiceprints*, Meta makes exactly that disclosure. Compl.
 20 ¶¶ 137–41; RJN, Ex. B at 4. That is in no way a disclosure that Meta *is* turning voice recordings into
 21 voiceprints. Indeed, if Meta were actually turning recordings into voiceprints, the allegation that it
 22 would disclose that conduct in a section of a notice expressly directed at complying with the laws of
 23 states *other than Illinois* is itself implausible. If anything, the Regional Privacy Notice supports the
 24 *more* plausible inference that Meta provides the required notice when state law regulates the
 25 information Meta does collect.

26 **2. Ms. Turck Does Not Plausibly Allege That Meta Collected Her Voiceprint**

27 Ms. Turck’s claims fail for another, independent reason: she piles a second unfounded
 28 inference upon the first. Even if the patents and the Regional Privacy Notice could support an inference

1 that Meta collects *some* voiceprints, the complaint fails to allege facts plausibly showing that Meta
 2 used these technologies *in connection with Facebook and Messenger, which Ms. Turck claims she used*.
 3 In describing her own experience, Ms. Turck alleges only that she “input her voice into an audio
 4 function on Facebook or Messenger . . . to dictate text messages to send via Messenger, sen[d] an audio
 5 recording of her voice via Messenger, and mak[e] audio calls via Messenger.” Compl. ¶ 149.

6 Neither the patents nor the Regional Privacy Notice can support an inference that Meta used
 7 voiceprint technology in connection with these particular services. The patents refer only to a
 8 hypothetical “social-networking system,” Compl. ¶¶ 56–64, not Facebook or Messenger, and they
 9 make no reference to the specific audio features that Ms. Turck alleges she used. Meanwhile, the
 10 Regional Privacy Notice covers many of Meta’s services, such as Instagram (including apps like
 11 Threads and Boomerang), Meta Portal-branded devices, Meta Platforms Technologies Products (such
 12 as Meta Horizon Worlds or Meta Quest), Shops, Meta Spark, Meta Audience Network, Facebook
 13 View, Meta Pay, and Meta Business Tools—not just the Facebook and Messenger services that Ms.
 14 Turck claims to have used. *See* RJN, Ex. B at 1–2 (Regional Privacy Notice supplements the Privacy
 15 Policy), Ex. A at 3 (Privacy Policy covers these services); Compl. ¶¶ 148–49.

16 And even if there *were* some way to tie the patents or the Regional Privacy Notice to the
 17 particular services that Ms. Turck alleges she used, there still would be no indication in the complaint
 18 that *her* voiceprint was collected. For instance, Ms. Turck does not (and cannot) allege that Meta in
 19 fact identified her by her voice. Rather, Ms. Turck alleges only that Meta collected her voice recording
 20 from the audio she input into Facebook or Messenger, Compl. ¶ 149, and then makes a huge logical
 21 leap to allege that Meta therefore “obtained [her] voiceprint,” *id.* ¶¶ 151–52. Because this assertion is
 22 not supported by any factual allegations, it amounts to a legal conclusion that is “not entitled to the
 23 assumption of truth.” *Iqbal*, 556 U.S. at 679; *see also Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d
 24 279, 285 (N.D. Ill. 2019) (dismissing BIPA claim under Section 15(d) where plaintiff alleged, without
 25 factual support, that defendant transmitted her biometric data to third party because the court “cannot
 26 allow [plaintiff] to proceed on such speculative allegations”).

1 **3. Ms. Turck Does Not Plausibly Allege That Meta Collected Her Voiceprint From**
 2 **Audio Recordings Provided By Any Third Party**

3 Even if Ms. Turck could plausibly allege that Meta collected her voiceprint—and she cannot—
 4 she certainly cannot plausibly allege that Meta collected her voiceprint from audio recordings provided
 5 to Meta by unnamed “third parties.” Accordingly, her claims must be dismissed insofar as they are
 6 premised on such allegations.

7 Ms. Turck alleges “on information and belief” that, independent of Facebook and Messenger,
 8 Meta received audio recordings from “third party sources,” such as unnamed “[c]ompanies or
 9 organizations” that do not use Meta’s services. Compl. ¶¶ 77, 81, 117, 124–25. She then asserts simply
 10 that she “believes that . . . *her* voice has been captured by Meta via” these third-party sources. *Id.* ¶ 150
 11 (emphasis added). From this, she speculates that “Meta created . . . [or] otherwise obtained [her]
 12 voiceprint.” *Id.* ¶¶ 151–52. But Ms. Turck never identifies any third parties who supply audio
 13 recordings to Meta, or explains why those third parties would have audio recordings of *her* voice. She
 14 also does not allege, much less plausibly allege, that any audio recordings these third parties supplied
 15 to Meta in fact included audio recordings of *her* voice. And she does not allege, much less plausibly
 16 allege, that Meta created *her* voiceprint from *that* third-party-derived audio content. This attenuated
 17 chain of speculation cannot sustain Ms. Turck’s BIPA claims under Rule 8. *Twombly*, 550 U.S. at 555
 18 (a plaintiff must plead “[f]actual allegations” that “raise a right to relief above the speculative level”
 19 under Rule 8); *see also Ctr. for Biological Diversity v. Bernhardt*, 946 F.3d 553, 560 (9th Cir. 2019)
 20 (holding that plaintiff did not allege facts to “‘nudge[]’ its claim of injury ‘across the line from
 21 conceivable to plausible’” where the “alleged injury rest[ed] on a speculative chain of future
 22 possibilities”).

23 Nor can Ms. Turck evade Rule 8 by pleading her third-party theory on “information and belief.”
 24 Compl. ¶ 77. “An allegation made on information and belief must still be ‘based on factual information
 25 that makes the inference of culpability plausible.’” *Menzel v. Scholastic, Inc.*, No. 17-cv-05499-EMC,
 26 2018 WL 1400386, at *2 (N.D. Cal. Mar. 19, 2018); *see also Scott v. Experian Info. Sols., Inc.*, No.
 27 18-CV-60178, 2018 WL 3360754, at *6 (S.D. Fla. June 29, 2018) (“[A]llegations stated upon
 28 information and belief that do not contain any factual support fail to meet the *Twombly* standard.”);

1 *Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 969 (N.D. Ill. 2020) (dismissing the plaintiff’s
 2 BIPA claim relying “solely on ‘information and belief’”). Here, Ms. Turck’s third-party theory is pure
 3 speculation and is not even specific to her. “Such barebone factual support . . . is not enough to put
 4 [Meta] on notice of [Ms. Turck’s] claims in order to properly investigate or prepare a defense.” *Kloss*
 5 *v. Acuant, Inc.*, 462 F. Supp. 3d 873, 877 (N.D. Ill. 2020) (dismissing the plaintiff’s BIPA claims for
 6 failure to state a claim under Rule 12(b)(6)).

7 Ms. Turck’s third-party theory is too speculative even for Article III standing. To satisfy Article
 8 III standing, a plaintiff must plead and show that she suffered an injury in fact that is “concrete and
 9 particularized” and “actual or imminent, not conjectural or hypothetical.” *Spokeo, Inc. v. Robins*, 578
 10 U.S. 330, 339 (2016). But Ms. Turck’s third-party theory is entirely conjectural and hypothetical. She
 11 pleads no legitimate reason even to suspect that third parties supplied Meta with audio containing *her*
 12 voice recording, and that Meta then used that audio to create *her* voiceprint. In other words, she has
 13 no plausible basis to allege how any third-party-derived audio affected her “in a personal and individual
 14 way”—a pleading deficiency that “will not do for standing.” *Zellmer v. Facebook, Inc.*, No. 3:18-cv-
 15 1880, 2022 WL 16924098, at *2–3 (N.D. Cal. Nov. 14, 2022). Because Ms. Turck “lacks Article III
 16 standing to pursue [her] . . . BIPA claim” based on third-party content, *id.* at *4, her claims cannot be
 17 sustained on a third-party theory, *see also, e.g., Dep’t of Educ. v. Brown*, 600 U.S. 551, 567 (2023)
 18 (rejecting standing theory where the “line of causation” between challenged action and plaintiff’s injury
 19 “is attenuated at best” and “all too dependent on conjecture” (internal quotation marks omitted)).

20 **C. Ms. Turck’s BIPA Claims For Profiting And Storage Fail For Additional Reasons**

21 Even if Ms. Turck could plausibly allege that Meta collected her voiceprint (and she cannot),
 22 her claims under Sections 15(c) and 15(e) of BIPA would still fail. Those claims allege, respectively,
 23 that Meta has “profited” from her voiceprint and failed to store or transmit her voiceprint securely. But
 24 she alleges no facts supporting these claims. For this additional reason, these claims should be
 25 dismissed.

26 **1. Ms. Turck Has Not Plausibly Alleged That Meta Profits From Her Voiceprint**

27 Ms. Turck fails to state a claim that Meta violated Section 15(c) of BIPA, which provides that
 28 no private entity in possession of biometric data “may sell, lease, trade, or otherwise profit” from that

1 data. 740 Ill. Comp. Stat. 14/15(c). Ms. Turck predicates her claim on allegations that Meta uses
 2 voiceprints to “improve its voice recognition and identification” technology and to “identify users so
 3 that it can send them customized, targeted content, including targeted advertisements.” Compl. ¶ 97;
 4 *see also id.* ¶¶ 185–86. She asserts that these activities have “allowed Meta to profit” in violation of
 5 Section 15(c). *Id.* ¶ 186. But, as a matter of law, Section 15(c) does not cover the activities she alleges.

6 When a statute, such as Section 15(c), includes a general phrase following a list of specific
 7 words, the general phrase is interpreted to include only things of the same type as what is listed. *See,*
 8 *e.g., Vance v. Microsoft Corp.*, 534 F. Supp. 3d 1301, 1306 (W.D. Wash. 2021) (construing Section
 9 15(c) of BIPA on a motion to dismiss). Here, the specific terms “sell,” “lease,” and “trade” inform the
 10 scope of the general phrase “otherwise profit.” 740 Ill. Comp. Stat. 14/15(c). Thus, “in the context of
 11 the enumerated terms, ‘otherwise profit’ encompasses commercial transactions—such as a sale, lease
 12 or trade—during which the biometric data is transferred or shared in return for some benefit.” *Vance*,
 13 534 F. Supp. 3d at 1307. In other words, Section 15(c) requires that the defendant “receive[] something
 14 of value” directly “in return for” access to the plaintiff’s data. *Id.*

15 This interpretation of “otherwise profit from” aligns with the legislative intent underlying
 16 BIPA. Section 15(c) creates a “general rule that prohibits the operation of a market in biometric
 17 identifiers and information.” *Thornley v. Clearview AI, Inc.*, 984 F.3d 1241, 1247 (7th Cir. 2021). But
 18 the Illinois legislature did not intend for BIPA “to stop all use of biometric technology.” *Vance*, 534
 19 F. Supp. 3d at 1307. Rather, BIPA set standards for ensuring safe collection and use of biometrics, in
 20 part to assuage “the public’s main fear that their biometric data would be widely disseminated.” *Id.* In
 21 the context of Section 15(c), then, BIPA “operates to remove one main incentive of sharing biometric
 22 data—to exchange it for some benefit.” *Id.*; *see also Thornley*, 984 F.3d at 1247 (Section 15(c) “flatly
 23 prohibits for-profit transactions.”). Thus, where a company sells, leases, or trades a biometric
 24 technology that “is so intertwined with [actual] biometric data”—like a facial recognition model that
 25 can identify people whose images were used to train the model—that conduct may run afoul of Section
 26 15(c) because “marketing the technology is essentially disseminating [the incorporated] biometric data
 27 for profit.” *Vance*, 534 F. Supp. 3d at 1309. But where a company merely uses biometric data to train
 28 or improve its products—even where the company “may have received some benefit from increased

1 sales of its improved products”—that conduct cannot give rise to a plausible claim under Section 15(c)
2 because it does not involve disseminating biometric data in exchange for consideration. *Id.*

3 In *Vance*, the district court applied this construction of Section 15(c) to dismiss a claim of
4 “profiting” that was materially indistinguishable from Ms. Turck’s claim. There, the plaintiff alleged
5 that “Microsoft used the [plaintiff’s] biometric data to ‘improve its facial recognition products and
6 technologies,’ which ‘improve[d] the effectiveness’ of those products and made them ‘more valuable
7 in the commercial marketplace.’” 534 F. Supp. 3d at 1309. “While these allegations support the
8 inference that Microsoft may have received some benefit” from the plaintiff’s biometric data, “these
9 allegations do not establish that Microsoft disseminated or shared access to biometric data through its
10 products,” or that “the biometric data is itself so incorporated into Microsoft’s product that by
11 marketing the product, it is commercially disseminating the biometric data.” *Id.*

12 The same analysis applies here. Although Ms. Turck parrots the statute in asserting that Meta
13 violated Section 15(c) “by selling, leasing, trading, or otherwise profiting” from her biometric data,
14 Compl. ¶ 190, she alleges no facts that could justify this conclusion. Even assuming the truth of her
15 allegations that Meta uses voiceprints to “improve its voice recognition and identification” technology
16 and to “identify users so that it can send them customized, targeted content,” *id.* ¶ 97, these allegations
17 would show only that Meta “may have received some benefit” from her biometric data—not that Meta
18 in any way disseminated that data for consideration. *Vance*, 534 F. Supp. 3d at 1309. As a matter of
19 law, such allegations are insufficient to state a plausible violation of Section 15(c). *See id.*

20 **2. Ms. Turck Has Not Plausibly Alleged That Meta Failed To Exercise Reasonable** 21 **Care In Storing Her Voiceprint**

22 Ms. Turck fails to state a claim that Meta violated Section 15(e) of BIPA, which provides that
23 a private entity in possession of biometric data must “store, transmit, and protect from disclosure” all
24 biometric data “using the reasonable standard of care within the private entity’s industry,” and “in a
25 manner that is the same as or more protective than the manner in which the private entity stores,
26 transmits, and protects other confidential and sensitive information.” 740 Ill Compl. Stat. 14/15(e).
27 Again parroting the statute, Ms. Turck asserts that Meta “failed to store, transmit, and protect from
28

disclosure” her voiceprint data in accordance with Section 15(e). Compl. ¶¶ 196–97. But again, she alleges no facts that justify this conclusion.

With respect to transmitting data or protecting it from disclosure, Ms. Turck never alleges that Meta actually transmitted or disclosed *any* voiceprint data. Thus, her claim necessarily fails on a transmission theory. *See Heard*, 440 F. Supp. 3d at 968 (dismissing Section 15(d) claim where plaintiff merely speculated that biometric data was transmitted); *Namuwonge*, 418 F. Supp. 3d at 285 (same); *Jones v. Microsoft Corp.*, ___ F. Supp. 3d ___, 2023 WL 130495, at *4 (N.D. Ill. Jan. 9, 2023) (dismissing Section 15(d) claim where the plaintiff merely “parrot[ed] BIPA’s language . . . [w]ithout more factual support”).

With respect to storage, Ms. Turck fails to allege any facts suggesting that Meta’s handling of her alleged voiceprint data fell short of industry or internal company standards. Ms. Turck does not allege what the “reasonable standard of care” is in Meta’s industry for storing voiceprint data. *See* Compl. ¶¶ 195–202. Nor does she allege how Meta is not meeting any such standard of care. *Id.* Ms. Turck also does not allege how Meta stores sensitive biometric data; nor does she allege how Meta is storing her alleged voiceprint data in a less protective manner. *Id.* The sole factual allegation in support of Ms. Turck’s claim is that Meta has acknowledged that—like any large company—it could be an attractive target for a cyber-attack, and that it was once the target of a cyber-attack. *Id.* ¶¶ 20–21; 198. But Ms. Turck’s allegations about the risk of a general cyber-attack say nothing about whether Meta allegedly stores *biometric data*—much less *voiceprints*—in a reasonably safe manner. Ms. Turck’s assertions therefore fail to nudge her Section 15(e) claim “across the line from conceivable to plausible.” *Iqbal*, 556 U.S. at 680 (quoting *Twombly*, 550 U.S. at 570).

V. CONCLUSION

The Court should dismiss Ms. Turck’s complaint with prejudice. Ms. Turck cannot pursue her claims against Meta, which arise from her use of Facebook and Messenger, under Illinois’ BIPA because she agreed to resolve any such disputes according to California law. Even if the Court were to decline to enforce the parties’ binding choice-of-law clause, Ms. Turck’s BIPA claims still fail because she has not plausibly alleged that Meta collects voiceprints at all, let alone from Ms. Turck specifically, through audio recordings collected from Facebook, Messenger, or any third-party sources.

1 At minimum, even if the Court concludes that Ms. Turck has plausibly alleged that Meta has collected
2 her voiceprint, her claims under BIPA Sections 15(c) and 15(e) independently fail because Ms. Turck
3 has not plausibly alleged that Meta profited from her supposed voiceprint or that Meta failed to store
4 and transmit her voiceprint using the appropriate standard of care.

5
6 Dated: October 25, 2023

GIBSON, DUNN & CRUTCHER LLP

7 By: /s/ Christopher Chorba
8 Christopher Chorba

9 *Attorneys for Meta Platforms, Inc.*
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28